2014

Cure Defense Enterprise IT Acquisition þÿ w i t h a D o s e o f i t s O w n M e d i c i

Gunderson, Chris

Cure Defense Enterprise Information Technology Acquisition with a Dose of its Own Medicine

Chris Gunderson, Naval Postgraduate School

Abstract— **The Defense Community's inability to realize its "enterprise" vision for the Global Information Grid (GIG) has reached crisis. The Defense Science Board (DSB) reports that a new acquisition process, aligned with commercial best practice is required. Commercial best practice is all about leveraging economy of scale to achieve better speed to better capability than the competition. Successful firms subscribe to a common model for value-based evolutionary development. The iPhone is good metaphor for that model. The JCIDS process can support the same model by morphing existing serial, paper-intensive compliance artifacts and processes into a continuous, parallel, automated process in a persistent virtual environment.**

I. DEFENSE ENTERPRISE INFORMATION TECHNOLOGY (IT) ACQUISITION BACKGROUND.

Per various watchdog reports, the Defense Community's inability to realize its "enterprise" vision for the Global Information Grid (GIG) has reached crisis.[1] The Defense Science Board (DSB) suggests information technology (IT) acquisition policy changes are necessary to mitigate the crisis. [2] Clearly, such policy should identify proven success criteria and best practices and incentivize adoption.

When it comes to large distributed, information-centric enterprises, the universal success criteria are better speed to better capability than the competition can deliver. Best practices are techniques for leveraging economy of scale and including customers as partners to continuously evolve an ever-improving value delivery chain. For example, successful practitioners such as eBay, iPhone, eFile, FedEx, and hundreds of others, employ the following model for value-based evolutionary acquisition:

- Business process improvement loop that includes customer-value-based lag metrics, transaction analysis, internal system performance lead metrics, beta development process, and a workflow optimization governance process that effectively couples these components to achieve enterprise objectives.

- Massively scalable, COTS, product line architecture built on routable Wide Area Networks (WAN) and Local Area Networks (LAN) and that seamlessly deliver value-added applications to decision making nodes.

- Federated governance model that includes objectively specified enterprise delivery "platform", branding criteria, and incentive model.

iPhone enterprise

To demonstrate, consider the iPhone "enterprise" from the perspective of an individual application developer, say Pandora Radio.[3] Federated governance includes agreement among app developers to use the iPhone platform. iPhone "Branding" means building to the various Apple proprietary specifications. The incentive is it is "cool" to be an iPhone app, plus you make lots of money from selling your app and/or from advertising that rides on top of your app.

Pandora Radio uses the massive scale of the World Wide Web to create automated personalized music streams for its subscribers. If the WWW did not exist, and if the various music providers were discoverable nodes, Pandora Radio could not succeed. Pandora did not invest to create the WWW or to create the music provider nodes.

The user-friendly Pandora Radio portal continuously collects input from the customer and refines output on the fly. Lead metrics are increasingly positive feedback regarding delivered musical choices. Lag metrics are advertising revenues.

Defense acquisition policy pays lips service to "commercial best practice" and evolutionary development of IT capability. However, acquisition policy directives overwhelmingly focus on compliance reporting rather than enforcing commercial best practices for IT systems engineering process. [4] The directives do not provide tools or incentives to encourage innovative or enterprise behavior. Not surprisingly, the resultant policy compliance artifacts are typically expensive, take a long time to develop, are delivered serially, and are redundant across stove-piped funding activities.

Nevertheless, some defense community activities have succeeded at value-based evolutionary acquisition. According to the Federal Acquisition Regulations (FAR) [5] "Acquisition" includes all the end-to-end activities associated with basic and applied research, developing, fielding, maintaining, and retiring capability. Successful value-based evolutionary acquisition among the defense community is most common during the maintenance phase of an IT capability life cycle. In those success cases, the government effectively peers with industrial providers to get good off-the-shelf value for its Operations and Maintenance (O&M) investments.

For modern information systems, "maintenance" is equivalent to "tech refresh". The objective of "tech refresh" is continuous improvement rather than continuous repair. Given that a primary objective of an "enterprise" approach is to leverage economy of scale, there should be no fundamental difference between "tech refresh", i.e. upgrading components of an existing shared infrastructure, and "developing" a new enterprise capability. In both cases the core infrastructure already exists and the objective is to quickly and continuously deploy improved capabilities.

In actual fact, a difference between "tech refresh" and "development" is the category of funding applied to each: O&M and RDT&E respectively. However, programs frequently apply RDT&E funds to rapidly deploy COTS as a "stop gap" in response to program schedule slips prior to Initial Operating Capability (IOC). That fact proves that there is no legal barrier to using a COTS tech refresh model to perform "development". Indeed, at least one major defense program, Acoustic Rapid COTS Insertion (ARCI) succeeded at that task as an overarching Acquisition Strategy. [6]

Having made the case that successful rapid evolutionary IT acquisition is possible in the existing defense community policy regime; the task becomes to make it common. The author's research suggests an approach to institutionalize best practices by creatively applying the existing defense acquisition policy compliance artifacts described in the Joint Capability Integrated Development System (JCIDS) manual.[7]

II. DEFENSE ENTERPRISE IT ACQUISITION PROCESS AS A JCIDS CAPABILITY

A. Online machine-readable Defense Enterprise IT acquisition policy directives and compliance reporting artifacts.

We can capture all defense acquisition policy directives in machine-readable form. For shorthand, use "Enterprise Policy Markup Language" (E-PML) to represent any number of semantic and/or modeling software languages adequate for the purpose. Cross check the various authoritative -- now machine-readable -- policy directives. Rationalize conflicts. Precipitate and parameterize the finite enforceable elements of policy. Generate E-PML acquisition compliance artifacts and provide them as Government Furnished Equipment (GFE) to the developer community.

An analogy is eFile tax return software. Complicated compliance requirements, i.e. the tax code, are programmed in "back-end" software. A simple online interface at the "front-end" collects required information. An online backend machine automatically checks for compliance and offers corrective guidance if/when necessary. Create re-usable defense community enterprise IT acquisition compliance artifacts as described in the following paragraphs.

B. Defense Enterprise IT Acquisition Capability Based Analysis (E-CBA).

Consider the Mar 2009 DSB report on IT Acquisition to be a JCIDS CBA addressing the need for an effective Defense Enterprise IT acquisition *process.*

Recognize that IT, and more specifically, software architecture together with communications transport,

provides the only means to compose semi-autonomous systems -- such as weapons, platforms, and sensors – into an Enterprise System of Systems (SoS). The existence of an enterprise, networked, SoS is obviously essential for effective, distributed, Command and Control (C2). This idea is the basis of netcentric theory and the GIG concept. Therefore, creating an effective Defense Enterprise IT acquisition process is a critical C2 issue…obviously.

The capability gap identified by the E-CBA is Defense Enterprise IT Infrastructure sufficient to realize the objectives of the GIG. That gap illustrates the need for a non-existent effective process. The E-CBA conclusion is to create such a process. That is, apply a non-material solution to address a critical capability gap. JCIDS guidance clearly encourages non-material solutions whenever possible.

C. Defense Enterprise IT Acquisition Process Initial Capability Document (E-ICD).

We can now precipitate an ICD for "Defense Enterprise IT Infrastructure Acquisition ***Process***" from the E-CBA. Define "Defense Enterprise IT Infrastructure" as federated routable wired and wireless Wide Area Networks (WAN) and Local Area Networks (LAN) together with a Common Computing Environment (CCE) including interoperable routable IT devices and value-added open standard enterprise software applications. Notice that Defense Enterprise IT Infrastructure is equivalent to Defense Enterprise Command, Control, Computers, Communication, Intelligence, Surveillance, and Reconnaissance (C4ISR) Infrastructure. Therefore, the purpose of the Defense Enterprise IT acquisition process is to enable value-based evolutionary development of continuously improving C4ISR infrastructure.

The E-ICD identifies a requirements gap for best business practices such as Defense Enterprise Business Process Analysis (E-BPA) and managed Defense Enterprise Workflow (E-Workflow)[8]. It also identifies the need for business process-level metrics, per best industrial practices.[9]

An "enterprise" is a federation of semi-autonomous organizations that each recognize the value of, and participate in, collaboration. In that spirit, note that the E-ICD does not address an individual acquisition program. Rather it provides a process for all programs to leverage, and or contribute to, Defense Enterprise IT infrastructure.

The concept of a Defense Enterprise is scalable. The enterprise concept can apply across all Defense Department, Intelligence Agency, and Law Enforcement Agencies, or, it can apply across any subset. These proposed Defense Enterprise IT Acquisition Process "JCIDS compliance" artifacts are designed to scale accordingly. Note that in this sense "compliance" means conforming to the minimum set of best practices agreed among members of a federation. Compliance is analogous to earning commercial logos such as ITIL, UL, Lean Six Sigma, CMMI, etc in that regard. Re-usable, machine-readable, user-friendly tools analogous to TurboTax enable "compliance". "Compliance" is in lieu of, rather than in addition to, the traditional paperwork-intensive approach. Therefore "compliance" with this new enterprise business process will be obviously useful to those who need to align subsets of individual programs, align programs across a particular military service, or align joint and coalition capabilities. See Appendix A: "Notional E-ICD."

D. Defense Enterprise IT Acquisition Process Architecture (E-PA), Information Support Plan (E-ISP), Key Performance Parameters (E-KPPs), and Reliability, Availability, and Maintenance (E-RAM).

Enterprise Process IT Architecture

Per the definition of Defense Enterprise IT Infrastructure offered in the description of E-ICD above, E-PA consists simply of wireless and wired WANS, that are connected by router to wired and wireless LANS, that are connected to routable devices, that execute enterprise applications, that seamlessly deliver value-added decision support services to decision making nodes. See Figures 1 and 2.

Enterprise KPPs

The mandatory Defense Enterprise IT Acquisition Process KPPs are the E- Sustainability KPP (E-S-KPP) and E-Net-ready KPP (E-NR-KPP).

The E-S-KPP is a process-level metric that equates "speed-to-capability" to "sustainability". In other words, the ability to rapidly and continuously refresh technology, including retiring superseded technology, is equivalent to sustainability of a modern enterprise information system. E-S-KPP is parameterized as "Availability of Net-readiness" (A_{nr}).

The E-NR-KPP is system-of-systems performance metric that defines net-readiness as a positive correlation between objectively measured Information Processing Efficiency (IPE) and Delivered Information Value (DIV). In other words,

the E-NR-KPP defines IPE in terms of a S-o-S's measured ability to improve desired operational outputs such as Probability of Kill (Pk), reduced fratricide, planning cycle compression, force readiness, etc. Reliability is an included aspect of IPE. E-NR-KPP is parameterized as "Availability of Information Value" (A_{iv}). See Appendix C: E-NR-KPP Formulation

The E-KPPs apply to individual program components. Rolling the aggregate of E-KPP performance across the programs of interest will provide an assessment of the Defense Enterprise IT Acquisition Process as a whole. Again, the overall objective is better-speed-to-better-capability. The following are alternative metrics to assess any subset of the Defense Enterprise against that broad objective:

- Better aggregate mission-outcome metrics
- Faster average speed to capability
- Reduced cost per capability delivered
- More predictable cost per capability delivered

Notice that reduced IT cost is not a business objective. The premise is that sustained investment in IT will result in improved business outcomes.

Enterprise RAM and ISP

It follows that the E-RAM high-level requirement is to continuously deliver measurably faster speed, to measurably better, capability. E-S-KPP and E-NR-KPP provide the measurement tools and framework for managing options.

The E-ISP, then, is the plan to address specific E-RAM requirements via continuous E-BPM and E-Workflow. See figure 6.

E. Defense Enterprise IT Acquisition Process Technology Development Strategy (E-TDS), Systems-of-Systems Engineering Plan (E-SEP), and Acquisition Strategy (E-AS).

Enterprise Technology Development Strategy

The main tenant of the E-TDS is to buy down risk by performing continuous COTS tech refresh to address as much of the total requirement as possible. Use E-BPA to identify the gap between delivered COTS capability and essential defense enterprise infrastructure requirements. Information Assurance (IA) and Semantic Interoperability (SI) are obvious gap areas. Invest Science and Technology (S&T) and Research and Development (R&D) funds to have COTS vendors iteratively close the gap in short spirals.

Systems Engineering Plan

Program Requirements: High-level requirements are defined in the E-CDD and E-CPD. Detailed requirements flow from continuous analysis of mission use cases, i.e. mission level workflow. That analysis is performed in partnership with operational practitioners and drives continuous refinement of the E-KPPs.

Testing and Certification will be performed per Testing and Evaluation Master Plan.
Technical Staffing and Organization Planning: E-SEP specifies that program technical staff and organization must include a Beta Development community of operational practitioners. Note that the same Beta Community members will support various programs' requirements. The approach must not over-burden operators. Rather, the enterprise IT infrastructure itself should include low friction tools for collecting Beta Community input.

Technical Baseline Management: Defense Enterprise IT Technical Baseline is mainstream COTS standards. Programs will use the E-S-KPP to measure and report compliance this baseline.

Program Technical Review Planning and Integration with Defense Enterprise Overall Management: E-workflow management tools will coordinate program developmental activity with designated technical compliance authorities.

Enterprise Acquisition Strategy

Per industrial best practice[10] the E-AS will favor Level of Effort (LOL) contracts -- wherein government and commercial partners share risks -- for software development. The E-AS will leverage the huge magnitude of the total Defense Enterprise IT investment to negotiate favorable terms with commercial providers. Negotiations will include non-traditional, approaches to managing Intellectual Property Rights (IPR) and Government Purpose Rights (GPR) across the Defense Enterprise. Elements of the E-AS include:

- Negotiating cost-effective means, beyond traditional license agreements, to distribute government-funded capability broadly as GFE
- Paying vendors to develop and maintain essential portable GFE infrastructure components, e.g. for IA and SI, under open source licenses.
- Service Level Agreements (SLA) and associated performance-based contract incentives tied to the E-KPPs.

- SLAs will including the requirement to establish Beta Development communities that include operational practitioners.

F. Defense Enterprise IT Acquisition Process Test and Evaluation Master Plan (E-TEMP).

The E-TEMP includes using E-Workflow to create a persistent virtual environment for continuing Test and Evaluation (T&E), Validation and Verification (V&V), and Certification and Accreditation (C&A) in parallel with small incremental developmental spirals, and in parallel across programs. For example, many programs need to integrate security services in context with similar information processing applications. E-Workflow tools can coordinate multiple programs' development activities together with the appropriate certification and approval authorities to perform IA certification in parallel.

Per Director of National Intelligence guidance[11] all Designated Approval Authorities (DAA) are required to recognize each others' certifications and accreditations. E-TEMP will address that requirement by publishing re-useable reference implementations of successful E-NR-KPP certification.

Net-readiness is a defense enterprise requirement. Per Chairman, Joint Chief of Staff CJCS direction [12] IA and SI are included aspects of net-readiness. Hence, E-NR-KPP certifications will objectively quantify IA and SI performance of the tested artifacts. We define IA as a SoS's ability to predictably and appropriately protect and/or make information available. We define SI as i.e. a SoS's ability to deliver actionable information to a decision-making node. Need-to-protect vs. need-to-share considerations are inherent in the E-NR-KPP formulation. See Appendix B: IA E-NR-KPP Template, and Appendix C: Semantic Certification Rationale. In this way E-NR-KPP certification can provide the basis of IA C&A for the appropriate DAA.

G. Defense Enterprise IT Acquisition Process Capability Development Document (E-CDD).

All the E-Acquisition artifacts described above inform the E-CDD. The E-CDD will explain how to create "federated governance" across the defense enterprise. This is largely a non-material, process-level, solution to implement the value-based evolutionary acquisition model described in the introductory paragraph. The E-CDD consists of the following conceptual components:

Business process improvement loop

The objective is to create a value delivery chain. A first step is to create an operational Beta Development Community to define "value" from the customer's perspective.

- Vendor SLAs require continuous "customer" feedback
- Use data collection tools embedded in "business" applications, per commercial model

Perform transaction analysis to define Valued Information at the Right Time (VIRT)

- Continuously capture operational use cases including mission threads, i.e. mission-level workflow
- Continuously audit E-NR-KPP performance, i.e. correlation between S-o-S performance lead metrics and mission outcome lag metrics

Create a persistent virtual development, T&E, V&V, and C&A environment to develop and demonstrate capability to deliver VIRT. (See Figure 3.)

- Regularly scheduled, e.g. quarterly, bundling events per published use cases including approval and certification authorities
- "Graduation" process for successful COTS/GOTS reference implementations to pre-approved product lists and Indefinite Delivery, Indefinite Quantity (IDIQ) and/or similar contract vehicles

Ubiquitous COTS Network Architecture

The Eventual goal is a "black core," i.e. a single point of entry to "the network" with multiple levels of access governed by dynamic Risk-adaptive Access Control (RAdAC)[13]

- Federated routable wired and wireless WANs and LANs
- Routable open standard devices
- Enterprise applications that seamlessly deliver value-added to decision making nodes.

Federated governance model (See Figure 4)

Specify Defense Enterprise network capability delivery "platform," i.e. Defense Enterprise network "Tier 0" specifications

- Unambiguously specified enterprise network "dial tone
- Universal access to persistent development environment

Establish "branding" criteria, i.e. a Defense Enterprise "Net-ready Logo."

- Pre-approved GFE components

- Objective E-KPPs
- Streamlined enterprise certification process

Establish a clear incentive model

- Level playing field across all of industry rather than traditional Defense "Cottage Industries"
- Reduced developers' costs for marketing to the Defense Enterprise
- Increased developers' speed to market
- Leverages government's research investments for commercial applications
- Patriotic opportunity to make a difference in an important cause

Return on investment

Again, aggregating performance against the E-KPPs across the components of enterprise should demonstrate:

- Better aggregate mission-outcome metrics
- Faster average speed to capability
- Reduced cost per capability delivered
- More predictable cost per capability delivered

See Appendix D: Notional E-CDD.

H. Defense Enterprise IT Acquisition Process Capability Production Document (E-CPD)

E-CPDs address tools for managing Defense Enterprise IT Acquisition business processes such as E-Workflow. E-CPDs also provide guidance for acquiring generic enterprise infrastructure components. As ever, emphasis is on off-the-shelf capability. Accordingly, the E-CPD is essentially a "living" consumer reports, catalog of pre-approved products, and "Craig's List" of providers and consumers of net-enabling capability. See Figure 5.

III CONCLUSION

We rank and file members of the Defense Enterprise owe it to the front line warriors to fix IT acquisition. We have all the policy we need to reverse our current unacceptable level of performance. However, we have to acknowledge that the approach to policy implementation that got us here will not get us out. We need to exercise enough courage and creativity to try another approach. In fact, we know what that approach is, because we use it every day when we go online to enrich our personal lives. Our enemy uses the same approach conduct effective C2 against us. So, in our case "the emperor" isn't really naked. He's wearing a ball and chain that he doesn't seem to see. We need to take it off him. He'll thank us.

IV REFERENCES

[1] OSD Directive to execute 180 day report on how to fix IT acquisition
[2] Defense Science Board, Mar 2009 report on IT Acquisition
[3] Pandora Radio website
[4] DODI 5000.02
[5] Federal Acquisition Regulations
[6] NPS ARCI Case Study
[7] JCIDS Manual
[8] Gartner Reference for BPA and Workflow
[9] GAO report on DoD Tech Transfer
[10] Reference for LoE contracting
[11] ICD 503
[12] CJCSI 6212
[13]NSA GIG IA Architecture

[1]

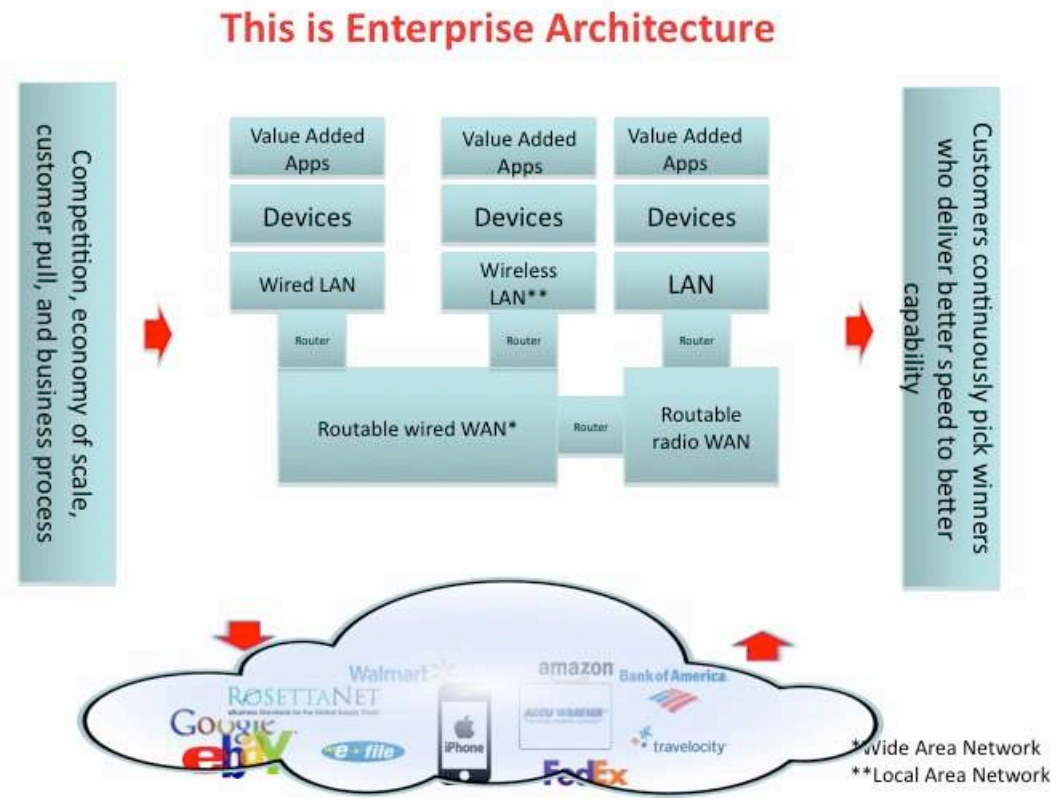

Figure 1: Enterprise Architecture in the Real World

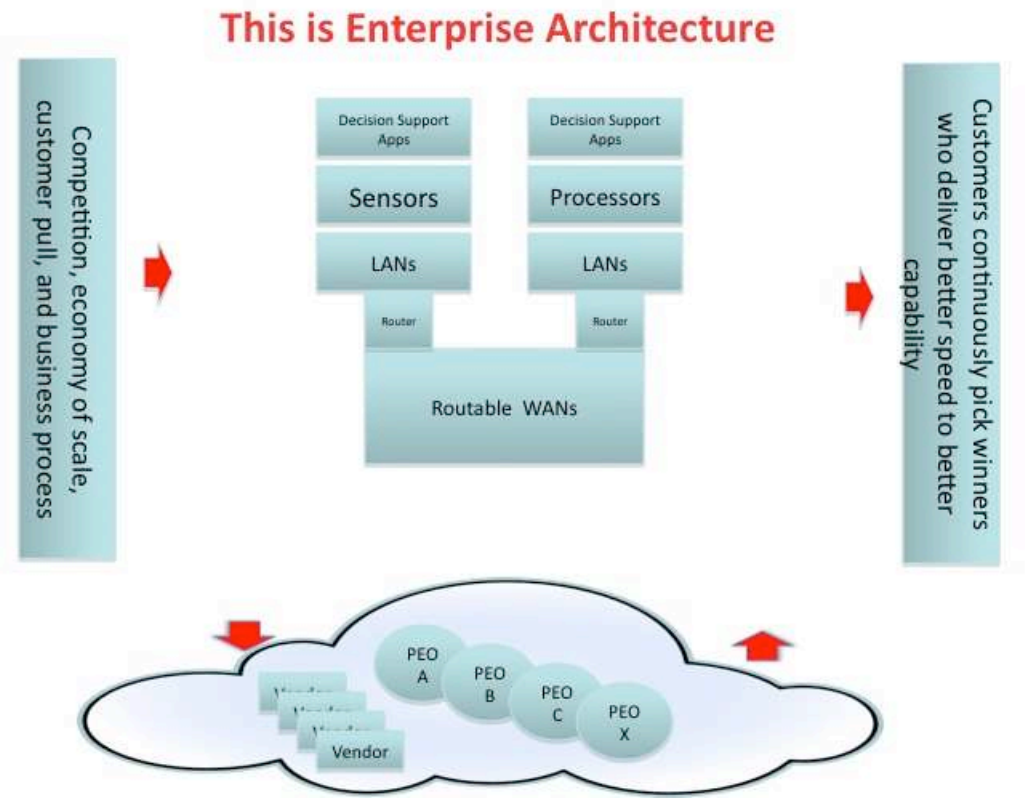

Figure 2: Defense Enterprise Architecture (if we finally get it right…)

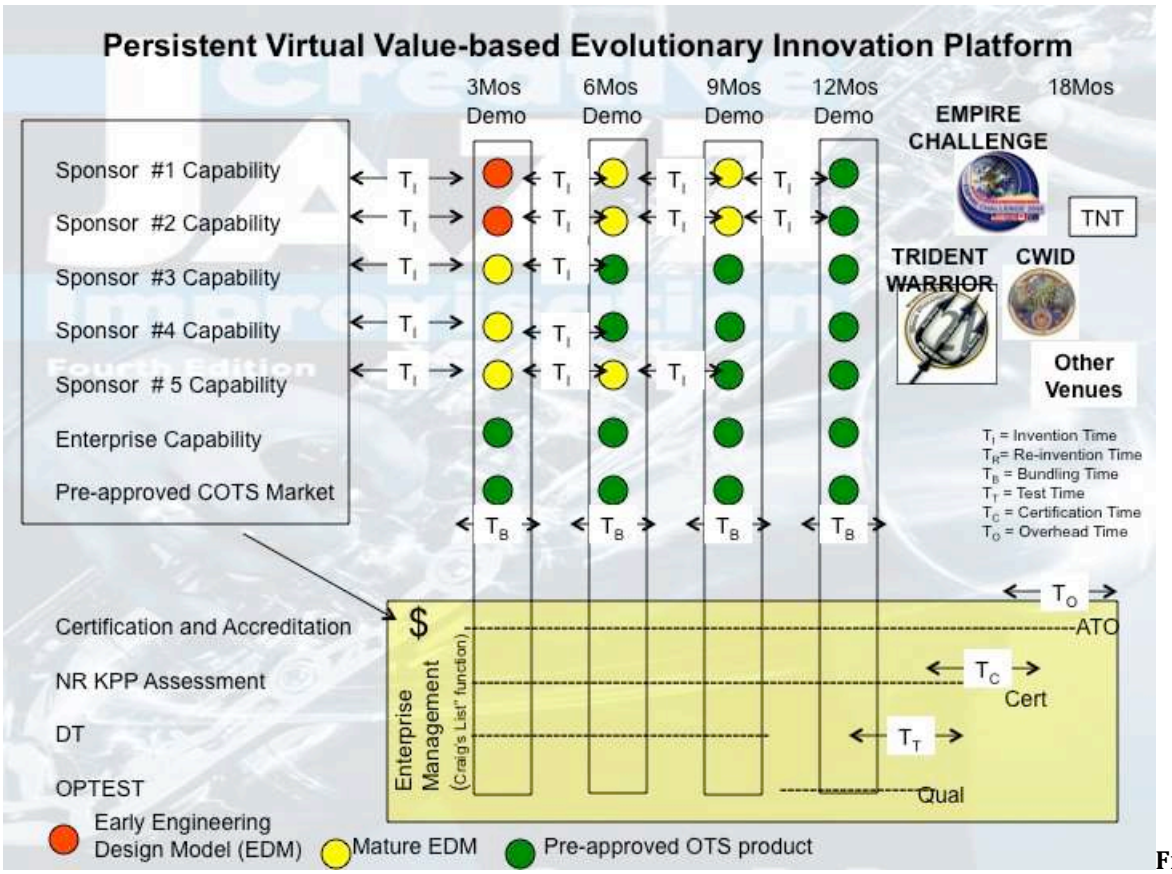

Figure 3: A Persistant D, T&E, V&V, and C&A environment and workflow management process. The "Enterprise" process is essentially a Craig's List resource to capture and share best practice, and broker providers and consumers of net-enabled capability.

Figure 4: Federated Governance Model

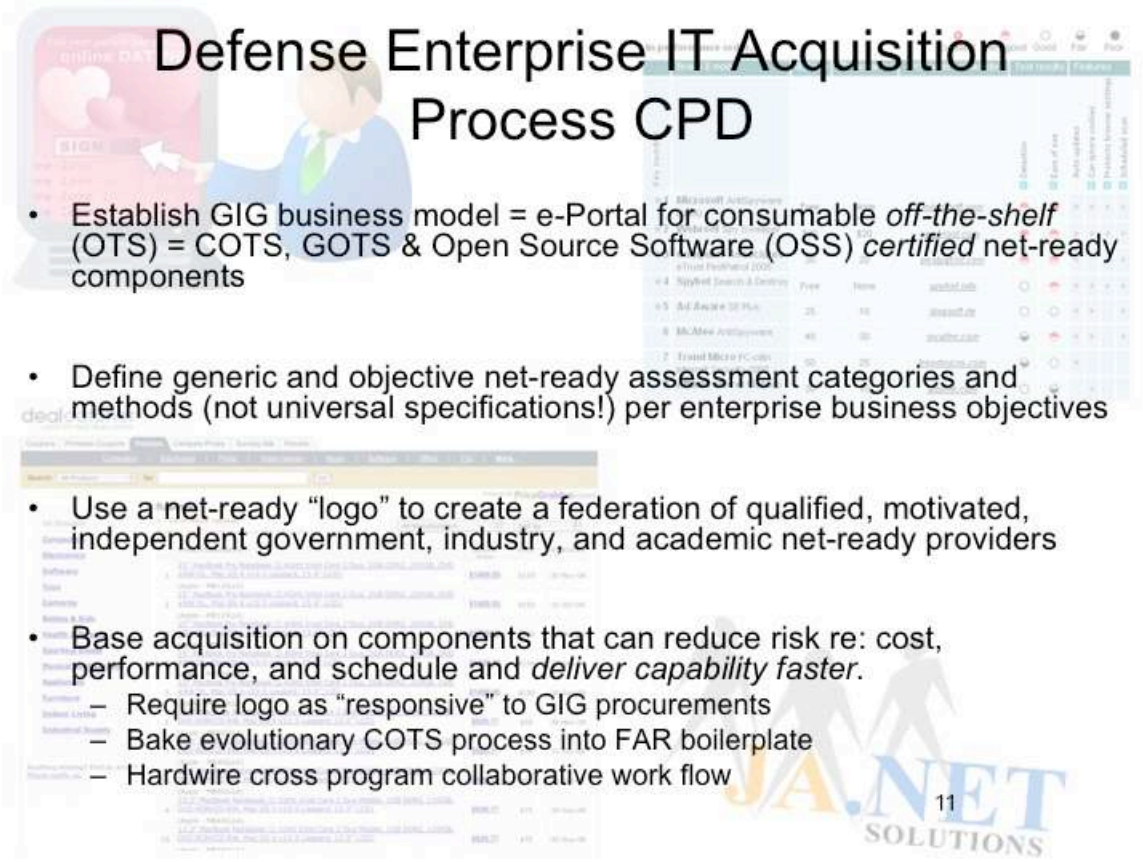

Figure 5: The Defense Enterprise Capability Production Document should be a portal to make it easy to consume enterprise-enabled capability. I.e., consumer reports + online test environment + brokering service + pre-approved online purchasing vehicle

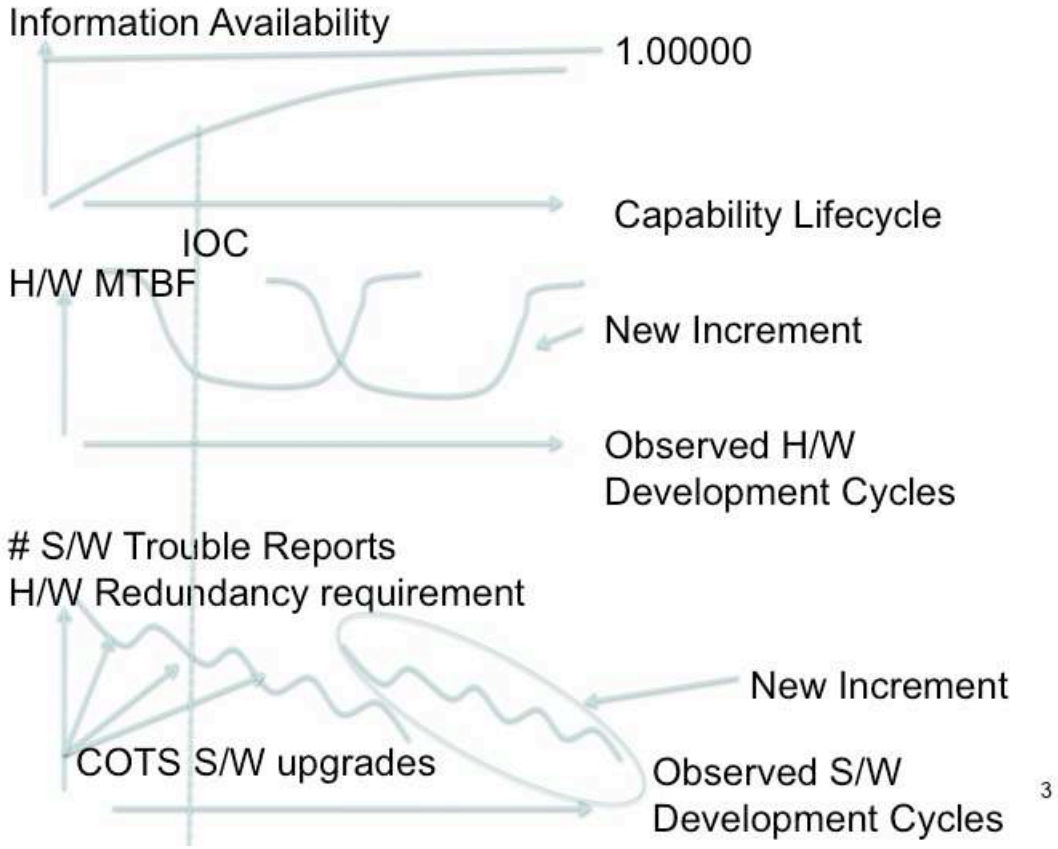

Figure 6: Enterprise RAM process should anticipate capability increase associated with enevitable software improvements. Deploy capabliity at threshold performance level. Manage improvment toward objective later in life cycle.

---

[1] OSD Directive to execute 180 day report on how to fix IT acquisition
[2] (Defense Science Board, 2009)
[3] Pandora Radio website
[4] DODI 5000.02
[5] Federal Acquisition Regulations
[6] ARCI Case Study
[7] JCIDS Manual
[8] Gartner Reference for BPA and Workflow
[9] GAO report on DoD Tech Transfer
[10] Reference for LoL contracting
[11] ICD 503
[12] CJCSI 6212
[13] NSA GIG IA Architecture